Proliferation of „Internet Governance“

Weber, Rolf H

INTERNATIONAL ISSUES: TRANSNATIONAL LEGAL TENSIONS AND INTERNET GOVERNANCE

Robert Faris and Rebekah Heacock Jones

The flow of data across international borders has been an undisputable engine of innovation in the digital economy and facilitated a myriad of tools, applications, and platforms used by citizens, businesses, and governments. Information freely flowing out of the reach of governments and without regard for international borders has long inspired cyber-utopians and cyber-libertarians. The questions of jurisdiction and control—whether governments should or could control the flow of information—have fueled debates over Internet governance and the role of government in digital affairs. While governments have done much over the past two decades to reassert their sovereignty in cyberspace, the complexities of regulating technologies that have little regard for geography continue to shape debates over Internet policy and governance. The relationship between national governments and Internet intermediaries constrains what a majority of Internet users are able to do on the Internet; only a relatively small cadre of users has the motivation and technological ability to overcome the technological limitations put into place by governments.

Where citizens use Internet services hosted domestically—social media, social networking, file sharing, blog hosts, email services, and others—the regulatory and jurisdictional questions are greatly simplified: governments are a phone call or subpoena away from gaining access to information needed to enforce local laws. The limited ability of governments to hold sway over foreign companies is a principal reason that the Internet is the way that is today. In China, authorities blocked access to western Internet services, including Twitter, Facebook, and YouTube, which helped to ensure that domestic alternatives control the market, giving the authorities the ability to enlist the help of intermediaries in policing content in a manner that outside companies would resist. The failure of YouTube and Twitter to respond to content filtering requests in Turkey led to the frequent blocking of those sites there. In Thailand, an agreement was reached with YouTube to block certain videos for Thai users that ran afoul of lese majeste laws, while these videos remained available elsewhere. Agreements reached with Google and Yahoo! enabled the removal of search results that pointed to content illegal in Germany and France, including hate speech and content related to Nazis. These agreements have formed the basis for broader systems to block content regionally where valid requests are submitted by legal authorities. These restrictions are notoriously flimsy—choosing an alternative country setting will gain access to the locally banned information—but offer an imperfect solution to a hard problem.

Efforts by sovereign governments to limit access to certain types of information within their borders and to secure user information housed in overseas servers will continue to strain this uneasy and constantly shifting equilibrium. The balance is maintained by adjustments to a small number of policy options: 1) maintaining international information flows by harmonizing standards across countries; 2) accommodations by international intermediaries to respect national differences; and 3) balkanization where these other two options fail. For countries around the world, the Internet has always been and will continue to be opt-in politically and socially. In terms of physical infrastructure and architecture, it continues to be opt-out; by default everything passes through the network unless measures are taken to create limits. Fortunately, there is a strong incentive for most countries to continue exchang-

ing information across borders using standard Internet protocols, which has limited the moves toward balkanization.

International power dynamics are impacted by the decisions of consumers and the ability of companies to attract users to their services. By virtue of the early and continued success of its technology companies, the United States has long held a favorable position, allowing it to maintain a strong stance of openness while also avoiding most jurisdictional problems and having access to user information when desired. The United States' commitment to safeguard free speech has been exported as the default option for other nations. By virtue of this trajectory, many countries have arguably allowed more online speech, accepted anonymous and pseudonymous speech, and permitted viewpoints that fall far enough outside of their social norms that they would not be tolerated in offline venues. The comingling of free speech with digital commerce has been a significant impediment to more decisively and comprehensively enforced national standards on acceptable speech. There continues to be a fair amount of friction in cross-border data requests, for example in the formal mechanisms in place to handle data requests across borders,[1] which has provided additional protection for many Internet users from their own governments.

The constantly evolving unilateral and bilateral arrangements between countries and companies determine most of the rules and standards for what passes across borders on the Internet, where servers with user data reside, and where company personnel are situated. Another complex set of policies and decisions are made at the international level that fall under the rubric of Internet governance. The set of issues cobbled together under this umbrella term generally includes the allocation of domain names, technical standards, and other areas related to technical coordination, and typically encompasses the activities of many organizations, including ICANN, IETF, IAB, W3C, and ISOC, among others. There is disagreement about the proper scope of Internet governance; some advocate for a narrow conception while others argue that it should include consideration of human rights as well as social and economic issues.

These Internet governance institutions are buoyed by the principles and practice of a bottom-up multistakeholder governance model. At its finest, multistakeholder governance is a sophisticated 21st century model that combines a thorough understanding and balancing of different interests and perspectives into an integrated decision-making process that enables consensus building around complex technological issues and brings to bear decentralized expertise. At its worst, multistakeholder governance is a fig leaf that conceals the back room deals that serve powerful interests and pay little heed to the interests of the broader global Internet community. This set of institutions and policies have held together and functioned reasonably well through the years despite unending criticism over the dubious legitimacy of the organizational structures by the standards of international law and weak mechanisms for ensuring accountability to the global Internet community. The system has sought legitimacy instead through process, primarily open participation and transparency, and outcome. While the imperfections of these governance institutions have been laid bare, it is not clear whether there are better alternatives in the offing.

The past year represents in some ways an existential crisis for Internet governance and its roots in multistakeholder governance. The pending expiration of a key contract with the United States govern-

ment has set in motion a search for modifying the current structure to better reflect the international responsibilities of ICANN.[2] (This contract is a core argument against the legitimacy of ICANN to make decisions of international import, and also a critical thread of comfort for those who worry that authoritarian governments will co-opt Internet governance in order to water down existing standards of openness and provide political support for greater content restrictions).

The Snowden revelations and the ICANN transition have sparked a surge in Internet governance-related activity. In October 2013, the leaders of the aforementioned Internet governance institutions released a statement on the future of Internet cooperation, warning against balkanization and calling for a sustained multistakeholder effort to address Internet governance issues.[3] Days later, after consulting with the President and CEO of ICANN, Brazilian President Dilma Rouseff—an outspoken critic of the NSA's mass surveillance programs—announced that Brazil would host an international conference on multistakeholder governance.[4] The conference, titled NETMundial, took place in April 2014 and brought nearly 1500 participants from nearly 100 countries. NETMundial resulted in a proposed set of essential principles for multistakeholder Internet governance and a "roadmap for the future evolution of the Internet Governance Ecosystem."[5] At the meeting, Rouseff also signed the Marco Civil da Internet, the Brazilian Civil Rights Framework for the Internet, into law. The roadmap presented during this meeting in Brazil has since formed the foundation for a range of high-level discussions of the future of Internet governance.

The state of international cooperation on Internet issues is in a state of flux. Many countries are advocating for a stronger role for multi-lateral institutions such as the ITU while others staunchly defend the merits of the multi-stakeholder model. The debates over legitimacy, principle, and practice in the coming year are destined to be impassioned. If the past serves as a reliable guide for the future, we should expect to see a mixture of unilateral, bilateral, and multilateral arrangements cobbled together atop an international network held together by rough consensus and running code. While far from perfect, this ad hoc legal, social, and physical architecture has fared remarkably well.

Notes

1 Sarah St. Vincent, "Coalition Urges Congress to Increase Funding for MLTA Process," Center for Democracy & Technology Blog, November 18, 2014, https://cdt.org/blog/coalition-urges-congress-to-increase-funding-for-mlat-process/.

2 Grant Gross, "U.S. government pulls out of ICANN," PCWorld, March 14, 2014, http://www.pcworld.com/article/2108780/us-government-to-end-formal-relationship-with-icann.html.

3 "Montevideo Statement on the Future of Internet Cooperation," ICANN Announcements, October 7, 2013, https://www.icann.org/news/announcement-2013-10-07-en.

4 "Brazil to host global internet summit in ongoing fight against NSA surveillance," RT, October 10, 2013, http://rt.com/news/brazil-internet-summit-fight-nsa-006/.

5 NETMundial Multistakeholder Statement, April 24, 2014, http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

The Rise of Information Sovereignty

Shawn Powers

Many have suggested the Internet's growth means (or should mean) the end of state sovereignty altogether. The logic behind such arguments is compelling. Technology has enabled citizens to create and join communities based not on geography, but on shared interests and ideologies, thus threatening the rationale for state-based nationalism altogether. Why would a citizen pledge loyalty to a state-based nation when a cornucopia of alternative communities that speak to specific interests beckon on the World Wide Web? According to this line of thinking, while states will certainly try to slow the transition, re-asserting their authority and legitimacy, globalization inevitably means the end of the nation-state as we know it.

At the same time, states control the telecommunications infrastructure that enables global connectivity. The physical nature of network connections allows any government to control information flow within its territory in a number of ways, including simply disconnecting its national communications infrastructure from all or parts of the global network. President Hosni Mubarak's decision to take Egypt entirely offline in 2011, as well as Edward Snowden's revelations regarding the existence of government-operated global surveillance apparatus, demonstrate just how vulnerable the web is to state control. Given the ease with which states can control access to the web, what is stopping governments from restricting access to the Internet? After all, even the father of international liberalism—Immanuel Kant—conceded states are motivated first and foremost by self-preservation.[1]

Information sovereignty refers to a state's attempt to control information flows within its territory. But control doesn't necessarily require a government to shut down access to the Internet. It is asserted in a variety of ways, including filtering, monitoring, and structuring industry-government relations in order to maximize state preferences in privately operated communications systems. A 2010 study by the OpenNet Initiative concluded that more than half a billion users—over a third of all users then on the Internet—experienced some form of filtering.[2] This does not include various measures to enforce copyright, prohibitions on hate speech, prohibitions on extremist propaganda, prohibitions on child pornography and exploitation, prohibitions on sales of controlled substances, or prohibitions on online gambling, all of which are enforced by a range of democratically oriented governments.

Monitoring, in particular, is an increasingly powerful means of asserting control over Internet-based communication. As more and more communication moves into the realm of the digital, government capacity to monitor private communication of all types increases. The digitization of information that is central to the Internet's functionality similarly eases government efforts to access, record, and share data from around the world. Drawing on Jeremy Bentham's articulation of the panopticon, Michel Foucault argues that the mere possibility of ubiquitous yet unconfirmed monitoring of a population is among the most effective ways of controlling behavior.[3] As users in Iran and China are well aware, Internet browsing and communication changes drastically when one thinks the government is watching.

Increasingly, both democratic and non-democratic governments are exploring ways to control access

to the Internet without losing legitimacy and, ultimately, power. For some states, access is only restricted in times of emergency, as was the case in Egypt in 2011. For others, access is systematically restricted, as is the case in Iran. China adopts a multifaceted approach, which includes draconian regulation as well as encouraging local, indigenous content creation. The United States is concerned about the consequences of depending on a shared, unsecured Internet, and is thus exploring variety of public-private partnerships in an effort to find the right balance between free speech and security. Denmark, on the other hand, is pioneering the use of digital tools to gain information on potential criminals, as well as cracking down on copyright violations.

Short of permanently cutting off all access to the Internet, governments around the world are exploring the different options for exerting control over domestic information flows. In some cases, these mechanisms allow for greater control over digital communications than was previously asserted over the analogue and interpersonal. Information sovereignty's emphasis on the political rights of governments to control information flows within their geographically delineated territories leverages two simple facts. First, the majority of the world's governments remain eager to protect and strengthen their sovereignty. Second, the majority of citizens support the nation-state system, holding on to nationalist views. As a result, information sovereignty is gaining traction, especially outside the West.

Notes

1 Immanuel Kant, Perpetual Peace, and Other Essays on Politics, History, and Morals, trans. by Ted Humphrey, (Indianapolis: Hackett Publishing Company, 1983).
2 Jillian York, "More Than Half a Billion Internet Users Are Being Filtered Worldwide," OpenNet Initiative, January 19, 2010, https://opennet.net/blog/2010/01/more-half-a-billion-internet-users-are-being-filtered-worldwide.
3 Michel Foucault, Discipline & Punish: The Birth of the Prison (New York: Vintage, 1995).

Boundless Courts and a Borderless Internet

Vivek Krishnamurthy

Ever since Yahoo! sparked a furor in 2004 by disclosing information to the Chinese government about the journalist Shi Tao's email account, which led to his arrest and imprisonment, major Internet companies have structured their operations in a jurisdictionally conscious manner to avoid contributing to human rights violations. Today, Internet companies service customers in some markets from servers located overseas so they can safely ignore requests from authoritarian governments to disclose user data. Similarly, companies often locate key personnel and data centers in jurisdictions with strong protections for civil liberties—in part to signal their compliance with rights-protective laws.

Two recent decisions by courts in established democracies against Internet company operations situated beyond their borders, along with the controversy surrounding the implementation of a third ruling, threaten to disrupt these arrangements, however—with potentially grave consequences for privacy and free expression should other courts adopt their logic.

The first is a decision in April by the federal district court in New York City commanding Microsoft to turn over to federal prosecutors the entire contents of a Hotmail account hosted at the company's Irish data center. Although US laws generally do not apply extraterritorially, the court found that the Stored Communications Act treats emails stored in the cloud as business records belonging to the service provider. As such, customer content stored anywhere in the world is subject to US court orders whenever the service provider operates in the United States. Microsoft is appealing the decision, arguing that the proper way for US law enforcement to obtain access to the Hotmail account is through the Mutual Legal Assistance Treaty with Ireland. Such treaties, which the US has signed with over 60 nations, allows law enforcement in one country to obtain the assistance of the authorities in another to collect evidence, among other forms of cooperation.

In a second case, a court in British Columbia (BC) levied a worldwide injunction in June barring Google from indexing entire domains associated with the sale of counterfeit versions of a company's products. While neither Google nor its Canadian subsidiary have employees or servers in BC, the Court held that it possessed jurisdiction over Google based on its sales of advertising to residents of the province. The Court conceded that most every court around the world would possess jurisdiction over Google on this base, but it nevertheless ruled that it could properly impose a worldwide jurisdiction against Google on the facts of this case, as the aggrieved company and the alleged counterfeiters had closer ties to BC than to any other jurisdiction.

Finally, there is the ongoing controversy over the interpretation of the European Court of Justice's decision in the "right to be forgotten" case, which held that European residents can have "inadequate," "irrelevant," "excessive," or simply outdated information about them de-indexed from search engines. Google in particular has responded to requests to be "forgotten" by de-indexing offending content from its European search offerings, such as Google.de and Google.fr. It has, however, kept such content available on Google.com as well as on its non-European search domains—all of which remain accessible within Europe. These actions have drawn the ire of European privacy regulators, who view

Google's failure to make such content entirely inaccessible in Europe as flouting the decision. No action has yet been taken against Google in this regard, but the possibility of further legal or regulatory action looms.

While courts in established democracies in North America and Western Europe might be trusted to wield extraterritorial powers responsibility, what happens when courts in countries that ignore the rule of law applies these precedents to its own ends? The New York court order to search Microsoft's Irish servers was issued by an impartial judge (mis)construing the rights protections in the U.S. Constitution, but what if a court in, say, Saudi Arabia were to issue a similar order against a company with employees on the ground there for account information stored in the United States? Similarly, what if the courts in Turkey or Thailand were to rule that videos and tweets mocking those countries' heads of states should be banned worldwide, and that they rightfully possess the jurisdiction to do so since their leaders enjoy a closer connection with their home countries than anywhere else? The result would be to reduce content on the Internet to the lowest global common denominator, or to balkanize the Internet into a set of regional networks within which local, rather than international, standards on digital searches and content suppression would prevail.

The current practice of the leading Internet companies to respect assertions of jurisdiction by governments within whose borders particular data is stored, or whose top-level domain graces a particular site, is not a perfect state of affairs. That said, it is far superior to a world in which governments everywhere can make demands of companies anywhere, backed up with the threat of sanctions against employees on the ground if they fail to comply. Regardless of the results in a particular case, courts in the world's established democracies should think carefully about the wisdom of setting precedents that are inherently extraterritorial—given their potential to be abused beyond their national borders.

The Great Firewall Welcomes You!

Nathan Freitas

In the last few years, usage of the mobile messaging app WeChat (微信), developed by Chinese corporation Tencent, has skyrocketed not only inside China, but also around the world. For 500 million mobile users in mainland China, WeChat is one of the only options for mobile messaging available, due to frequent or permanent blockage of apps like WhatsApp, Viber, Line, Twitter, and Facebook. For over 100 million mobile users in the rest of the world, a highly polished user experience, celebrity marketing, and the promise of "free calls and texts" has proven to be nearly irresistible for far-flung members of the Chinese diaspora. This global userbase also includes the Tibetan exile diaspora, who through WeChat have become connected on both sides of the Himalayas in near real-time like never before.

Instead of Chinese users scaling the wall to get out, people around the world are walking up to the front gate, knocking on the door, and asking to be let in. Just as you might expect with a service like WhatsApp or Twitter, every time you send a message on WeChat it is routed through centralized servers, managed by Tencent. In most cases, these servers are located inside of China, often in Shanghai-based data centers, though in some countries, local servers are being set up. These servers, though, are still within reach of Chinese law, regulations, and influence, and all data passing through them is vulnerable to surveillance and censorship.

The first concern is that China's demand for censorship of particular topics and keywords will begin to extend beyond its borders. As detailed analysis from the Citizen Lab's Asia Chats study has shown, censorship keyword lists can vary by geography.[1] If you mention "Occupy Central" in a message sent from WeChat in Beijing to someone in Chengdu, it will likely be blocked and your profile flagged. If you send the same message using WeChat in Toronto to someone in New York, the message will likely go through, though your profile will most likely still be flagged.

The second concern is that communications by a user outside of China, be they a Chinese citizen or not, can be surveilled, logged, and used against them in the future. If you are in San Francisco, and you join a WeChat group chat that is sympathetic to Tibetan self-immolations or the Uighur community, and some members of that group are located in Tibet, Xinjang, and China, then all of your messages and the fact that you are participating in that group chat are communicated to servers managed by Tencent, licensed under the authority of the Chinese government. Since your WeChat account is tied to your real phone number and SIM card, and your full address book is accessible by the app, then your real name and entire community are now flagged as being sympathetic to groups that China considers as harmful as the Islamic State or Al Qaeda. Good luck getting a visa!

The third concern is that this type of service can be used for wholesale extraction of data and insertion of malware into targeted devices. Like most social media apps, the WeChat app on iPhone and Android has full permission to activate microphones and cameras, track your location, access your address book and photos, and copy all of this data at any time to their servers. These types of capabilities are a godsend to attacks known as a RAT (Remote Access Trojan), and usually have to be

snuck onto a laptop through infected PDF files. In the case of WeChat, the user is opting in to these capabilities, entrusting what may be a well-meaning social messaging service with "god mode" while unknowingly providing an easy backdoor on their phone for adversaries higher up the Chinese cyber-war food chain.

Illustration by Willow Brugh

Combined with the rise of attractive, low-cost mobile handsets from Huawei and Xiaomi that include China-based cloud services, which are being sold in India and elsewhere, the world is witnessing a massive expansion of Chinese telecommunications reach and influence, powered entirely by users choosing to participate in it. The fundamental question is: do the Chinese companies behind these services have any market incentive or legal obligation to protect the privacy of their non-Chinese global userbase? Do they willingly or automatically turn over all data to the Ministry of Public Security or State Internet Information Office? Will we soon see foreign users targeted or prosecuted due to "private" data shared on WeChat? Finally, from the Glass Houses Department, is there any fundamental difference in the impact on privacy freedom for an American citizen using WeChat versus a Chinese citizen using WhatsApp or Google?

For those of us in the global community who care both about ensuring that all humans can be more interconnected and provided free, unlimited access to knowledge, while also ensuring their privacy and dignity is protected, these are primary issues we must study, understand, and take action on. The next 5 billion people on Earth tend to live in more repressive places than free ones, and we must ensure that their desire to be connected in a "free and unlimited way" does not leave them in a virtual panopticon.

Notes

1 Citizen Lab, "Asia Chats: Analyzing Information Controls and Privacy in Asian Messaging Applications," November 14, 2013, https://citizenlab.org/2013/11/asia-chats-analyzing-information-controls-privacy-asian-messaging-applications/.

Toward an Enhanced Role of Academia in the Debates About the Future of Internet Governance—From Vision To Practice

Urs Gasser

Academics, academic institutions, and academic values have played a key role in the development of the Internet as well as in its operation and in what we today call "governance," especially at the logical layer consisting of technical standards and protocols. Indeed, it is impossible to imagine the Internet as we know it without the defining role academics have played since its inception in the 1970s. Similarly, core academic values such as openness, collaboration, and trust have inspired the early approaches to and initial modes of Internet governance, and have shaped its evolution since the 1990s. Important traces of these academic origins are still reflected in today's multi-stakeholder Internet governance ecosystem, which has come under significant pressure since the World Summit on the Information Society (WSIS)[1] in 2003 and 2005 and, perhaps most visibly, at the 2012 World Conference on International Telecommunications (WCIT-12).[2]

The contested policy debates that currently take place across various national and international forums—from NETmundial[3] to the ITU's 2014 Plenipotentiary Conference[4] and WSIS+10,[5] to name just a few—suggest that we have arrived at crossroads in the debates about the future of Internet governance. In the light of today's heated debates, this essay argues that it is timely to reflect on academia's role in the development and operation of the Internet over the past two decades and to renew its commitment to contribute systematically and from diverse perspectives to the Internet governance debates over the next decade. Second, it proposes an enhanced role of academia as we design the next-generation Internet governance model—a role that builds upon past contributions but is also based on a generalized vision and strategy regarding the importance of academic research, facilitation, experimentation, and education. Such an enhanced role emphasizes academic values such as independence, rigor, openness, and global participation. Before outlining the contours of an enhanced role of academia, let us turn to the question: why we should re-imagine the role of academia, and why now? The short answer is: because there is critical need, and because there are opportunities we should embrace.

Since the early days of the Internet governance, the world has changed dramatically, and so has the academic environment. When ICANN was founded in the late 1990s with the help of researchers at the Berkman Center, for instance, only a handful of academics were researching Internet and society issues. Today, Internet studies—or Internet science, as it is labeled in Europe—has evolved from an academic niche area (typically researched at law schools, given the porous methodological boundaries of law as a discipline) into an academic discipline in its own right, with emerging research methods, specialized journals, degree programs, chairs, and centers. We see more and more young people—master students, doctoral students, and so forth—interested in this growing field of research and work, most of whom share a strong interest in and commitment to interdisciplinarity. Similarly, it is no longer the stereotypical group of "white males in their 60s" actively addressing Internet governance issues, broadly defined, but an increasingly diverse community of scholars, researchers, and activists—many of them talented women and young people from the Global South. This generational shift, the increased diversity in terms of gender, orientation, and geographic representation, the com-

mitment to interdisciplinary, and novel institutional support structures provide a unique opportunity for coordinated and sustained academic collaboration on issues related to Internet governance that we should harness, adding perspectives from other domains, incubating alternative approaches and models, and re-energizing the great work previous generations of academics have contributed.

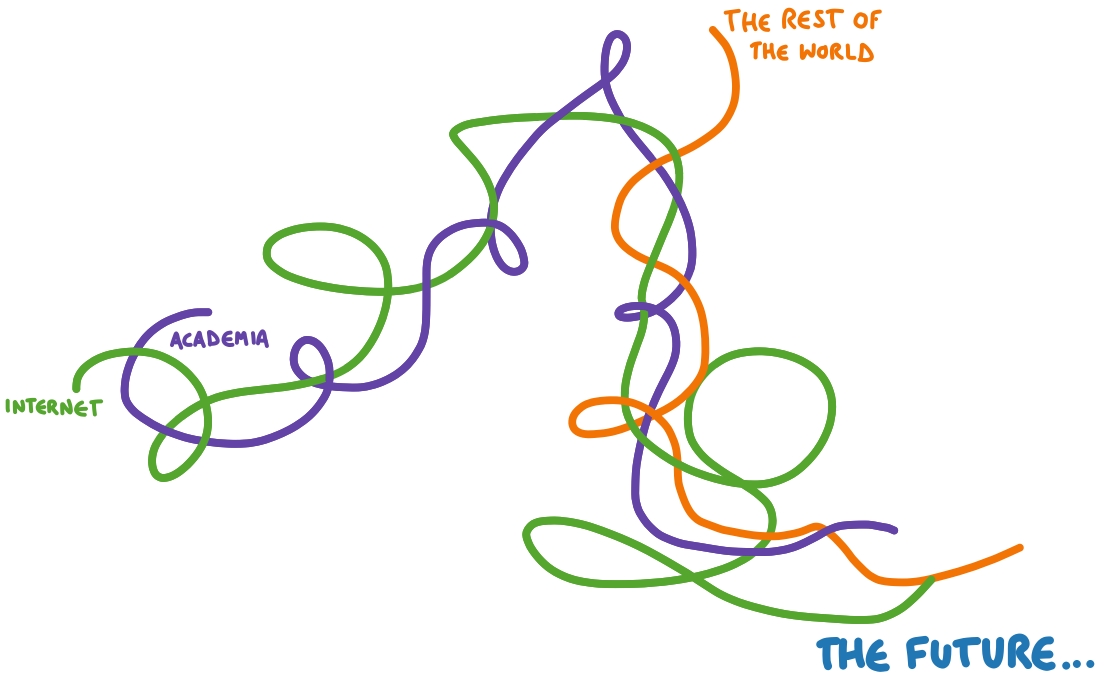

Illustration by Willow Brugh

It is not only opportunity, but also increased and pressing need that calls for a renewed commitment of academia based on a broader vision and strategy concerning its future role in the global debates about the future of Internet governance. It is commonly understood that the Internet now affects almost every aspect of life, that its governance has become more complex, and that the stakes are much higher than they were two decades ago. Controversies about multilateral versus multi-stakeholder approaches to Internet governance as well as the battles over a diverse set of issues (ranging from surveillance to intellectual property) are manifestations of the importance of the Internet as the core information and communication infrastructure of the digital age. In such a contested and highly politicized environment, it is vital to build upon, expand, and accelerate past academic efforts by broadening and coordinating the scope of inquiry, working towards institutional approaches, and developing global capacity. There is an increasing demand across all stakeholders for independent and rigorous research and scientific data, as well as for best practices and general principles that are created collaboratively and in the spirit of the academic values mentioned before. Viewed from such a perspective, academia can and should be more than a "stakeholder" in today's Internet governance debates. It is well-positioned to play a constitutive role as we develop a new vision of a next-generation Internet governance ecosystem in a time when governance debates are often ideological, fragmented, and mostly interest-driven rather than evidence-based.

At this critical juncture and in the light of new opportunities and pressing demands related to Internet governance, what could an enhanced role of academia look like in practice? A concrete example and

precursor in this context is a recent initiative by the Global Network of Internet & Society Research Centers,[6] which was incubated by the Berkman Center, built bottom-up, based on international collaborations, and formally launched in 2012. It now brings together more than 30 academic centers[7] with focus on Internet and society issues from around the globe, including nine members from the Global South. The network represents a broad range of disciplines, bridges many traditions and cultures, and engages many young as academics from diverse geographic backgrounds. As an evolving and learning network, it represents some of the key elements of the enhanced vision mentioned before, including the emphasis on institutional approaches and global capacity development, interdisciplinary research and building, systematic and sustainable engagement, and the engagement of new perspectives and talents.

In addition to these structural elements, an enhanced role of academia also calls for a concerted and sustained thematic engagement across the various layers of Internet governance research. Consider the following three questions as an illustration of the breadth of the issues that need to be addressed on different layers (others could be added):

- Data and research layer: What can we do, as a network of academic institutions, to create a global interoperable data platform to measure the Internet's health, which could serve as an information backbone for Internet governance research and decision making, providing high quality and open data to distributed Internet governance groups?
- Normative layer: How can academia serve as a "protected space" to develop the necessary normative foundations of future Internet governance models and mechanisms and facilitate difficult value conversations among Internet governance stakeholders, working towards consensus, good practices, and general principles of Internet governance?
- Design layer: Building upon research activities and conceptual studies, how can we as an academic community work together—in interdisciplinary teams and across departments, schools, and centers—to develop new institutional designs, experiment with new tools, and create new code or Internet governance?

These three examples indicate not only the broad range of possible contributions, which together with other elements might serve as the foundation of a holistic concept of Internet governance, but also point to the different modes of academic engagement in the multi-faceted Internet governance processes. The envisioned core pillars to which the examples partly allude, but need to be fleshed out elsewhere, include research, facilitation, experimentation, and education (encompassing also skill building and practical training).

The partnership between the Berkman Center and the Network of Centers and the engagement of this institutional network in the current discussions about the future of Internet governance through a coordinated events series[8] and a research pilot[9] are intended as an initial step towards operationalization of the broader strategy and underlying vision as sketched in this essay. The Network of Center's research pilot consists of a case study series as building blocks of a synthesis document aimed at deepening our understanding of the formation, operation, and effectiveness of distributed Internet governance groups. The research examines a geographically and topically diverse set of local,

national, and international distributed governance models, components, and mechanisms from within and outside the sphere of Internet governance. With its initial focus on emerging lessons learned and (contextual) good/best practices, the goal of the research pilot is to inform the evolution of the Internet governance ecosystem in the light of the NETmundial Principles and Roadmap, the discussions at the Internet Governance Forum (IGF), and other forums, panels, committees, and initiatives.

In parallel to weighing in on these and related conversations about the next-generation Internet governance models and mechanisms, academia has a responsibility to re-envision its own future in this zone, reflecting and building upon the great contributions of the past. The months and year to come will provide a unique window of opportunity to further flesh out the proposed vision and strategy for an enhanced role of academia, incorporating lessons learned from current efforts and pilots. Contributions by the Network of Centers, as well as related efforts such as the Global Internet Governance Academic Network (GigaNet[10]) and the Research Advisory Network (RAN) to the Global Commission on Internet Governance, are important building blocks in this respect. But working from vision to practice will require not only collaboration among academic networks around the globe. Success will also depend on longer-term commitments by leaders in the public and private sector as well as open participation of civil society actors. Realizing the promise of an enhanced role of academia is a shared responsibility as we build together an Internet governance system for future generations.

Additional Reading

DeNardis, Laura. The Global War for Internet Governance (New Haven: Yale University Press, 2014).

DeNardis, Laura, and Mark Raymond. "Thinking Clearly About Multistakeholder Internet Governance," SSRN, November 14, 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2354377.

"Developing Meaningful Multistakeholder Participation Mechanisms," IGF 2014 Best Practices, Internet Governance Forum, 2014, http://review.intgovforum.org/igf2014/best-practices/developing-meaningful-multistakeholder-participation-mechanisms/.

Drake, Bill, and Monroe Price, eds.. Beyond Netmundial, August 2014, http://www.global.asc.upenn.edu/app/uploads/2014/08/BeyondNETmundial_FINAL.pdf.

Dutton, William H., ed. The Oxford Handbook of Internet Studies (Oxford: Oxford University Press, 2013).

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. Brief History of the Internet, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

Mueller, Milton. Networks and States: The Global Politics of Internet Governance (Cambridge: The MIT Press, 2010).

"NETmundial Multistakeholder Statement." Global Multistakeholder Meeting on the Future of Internet Governance, Rio De Janeiro, Brazil, April 24, 2014, http://netmundial.br/netmundial-multistakeholder-statement/.

Palfrey, John, and Jonathan Zittrain. "Better Data for a Better Internet," Science 2 December 2011, Vol. 334 no. 6060 pp. 1210-1211, http://www.sciencemag.org/content/334/6060/1210.full?ijkey=yLssWDbbr0ekI&keytype=ref&siteid=sci%2520.

Radu, Roxana, Jean-Marie Chenou, Rolf H. Weber, eds.. The Evolution of Global Internet Governance. Principles and Policies in the Making (Berlin: Springer, 2013).

Waz, Joe, and Phil Weiser. "Internet Governance: The Role of Multistakeholder Organizations". Journal on Telecommunications & High Technology Law, 10, (2012): 331, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2195167.

Weber, Rolf H. Regulatory Models for the Online World (Berlin: Springer, 2002).

---. Shaping Internet Governance: Regulatory Challenges (Berlin: Springer, 2009).

Notes

1 World Summit on the Information Society, http://www.itu.int/wsis/index.html.
2 2012 World Conference on International Telecommunications, http://www.itu.int/en/wcit-12/Pages/default.aspx.
3 NETmundial, http://netmundial.br/.
4 ITU Plenipotentiary Conference 2014, https://www.itu.int/en/plenipotentiary/2.
5 WSIS+10, http://www.itu.int/wsis/review/2014.html.
6 Global Network of Internet & Society Research Centers, http://networkofcenters.net/.
7 "Participating Centers," Global Network of Internet & Society Research Centers, http://networkofcenters.net/centers.
8 "Events," Global Network of Internet & Society Research Centers, http://networkofcenters.net/events.
9 "Research," Global Network of Internet & Society Research Centers, http://networkofcenters.net/research.
10 GigaNet, http://giga-net.org/.

Proliferation of "Internet Governance"

Rolf H. Weber

According to a well-known description, Internet Governance "is the simplest, most direct, and inclusive label for the ongoing set of disputes and deliberations over how the Internet is coordinated, managed, and shaped to reflect policies."[1] In other words, Internet Governance "evolves" the design and administration of the technologies necessary to keep the Internet operational and facilitate the enactment of substantive policies around these technologies.[2] Such design requires the fructification of law as instrument structuring an order in the public interest.

1. Functions of law

The functions of law crystallize in a system of rules and institutions that underpin civil society, that facilitate orderly interaction, and that resolve disputes and conflicts arising in spite of such rules. Law can be created by way of negotiation, imposition, and evolution. In cyberspace, the evolutionary aspect is of major importance since new concepts are developing, for example through the creation of normative principles or the implementation of "rules" derived from codes of conduct, corporate social responsibility, and other similar initiatives.

Law is able to regulate behavior, and it allows people in a community to determine the limits of what can and cannot be done in their collective interest. Law as a structural system is traditionally featured with coercive effect.[3] If law is properly implemented, its provisions can be enforced against the will of individuals. However, irrespective of its (coercive) quality, the legal system is embedded in other socially relevant systems; in particular, "cyber-norms" depend on social norms.[4] Developments in technology and/or society, expressed in informal standards, can and should give input to legislative bodies; thereby, the acceptability of legal norms increases if they are based on informal social standards that are derived from customary behavior of civil society.[5]

The relativity of norms reflecting civil society's needs is evidenced by the fact that norms can come in a variety of shapes with different effects; insofar the legal system is linked to other social sub-systems and executed through a framework of structural couplings.[6] Such kind of structure calls for a multilayered approach in norm-setting.[7]

When designing the future cyberspace legal framework[8] the fact should be considered that architects are the experts in sketching "constructions." More than a hundred years ago, the famous architect Louis H. Sullivan said: "It is the pervading law of all things, organic and inorganic, of all things, physical and metaphysical, of all things human and all things superhuman, of all true manifestations of the head, of the heart, of the soul that the life is recognizable in its expression, that form ever follows function. This is the law."

Sullivan uses the word "law" twice while attributing the notion of making form dependent on function. Therefore, when designing a global Internet Governance framework, the function of law has to be considered in more depth; following Bentham's principle of utility and Luhmann's approach of

stabilization of normative expectations, a functional approach that bodes for the political design of Internet Governance should determine the normative order.

As a result, the main question could be phrased as follows: What social impacts should be caused by law? The answer is based on the expectations of civil society. These expectations change over time, but some elements remain the same, such as legal certainty, stability, and reliability. In times of fast developing information technologies, civil society is better able to rely on these principles in an informal law-making process and context than in the traditional legal regime.
Thesis 1: A functional approach of rule making is necessary to adequately capture socio-political expectations of civil society.

2. Increased dynamics through socio-technological developments

Technological developments in the information and communication field, particularly the process of digitization, have caused advances that lead to widespread social change.[9] These advances need to comply with at least three social expectations:[10] (i) applications for the public have to be available from a technical point of view; (ii) applications and projects leading to them must be socially and commercially acceptable; and (iii) the implementation and usage of the systems should be done such that they are achievable from a cultural perspective.

In the Internet context, technological developments require an adaptation of the regulatory design and its modalities, which can be differentiated into socially-mediated modalities and environmental modalities. Thereby, the regulatory authority called upon to settle a regulatory disruption may choose to "utilize any of the socially mediated modalities either alone or in a hybrid regulatory model."[11] Correspondingly, modern socio-legal theory has tried to develop models that ideally should overcome legal instability. As a consequence, the legal framework should encompass the socially desirable requirement that netizens be members of civil society and should simultaneously become manageable, available, realistic, workable, and interwoven easily with all aspects of social life.

These developments caused by technologies and influencing the social/environmental parameters of an open society make the regulatory systems more dynamic. Cyber-communities are successfully able to shape their internal relations with non-legal tools (technical standards, terms of use, codes' of ethics).[12] Therefore, regulators have to take into account the assessments of network engineers and communication theorists pointing to the vital function played by environmental layers in communications networks even if such approach leads to a complex structural matrix.[13]

Scholars have tried to capture these increased dynamics with a "global experimentalist governance" theory ("GXG"). An ideal GXG regime comprises five key steps,[14] namely: 1) initial reflection and discussion among stakeholders; 2) articulation of a framework understanding with open-ended goals; 3) implementation of these broadly framed goals; 4) continuous feedback provided from local contexts; and 5) periodic and routine re-evaluation of the goals and practices (including their possible adaption or revision). Certain similarities of the GXG approach with the multi-layer or network governance model do exist; however, GXG puts more emphasis on new forms of learning. A condition for GXG is

that States are unable to formulate a comprehensive set of rules and effectively monitor compliance. Furthermore, States must not be stymied by disagreement over basic principles, and the cooperation of civil society actors either as agenda setters or as problem solvers is normally indispensable. A problem with the GXG approach exists in its vulnerability to manipulation and unintended consequences, even if GXG has the potential to increase participation in, and thus the democratic legitimacy of, institutions. Additionally, the foreseeability and the predictability of legal norms are low, and a link to the international legal setting is missing.

Thesis 2: A stable Internet Governance framework can only be established if the respective rules reflect the socially desirable and manageable requirements of the civil society's members.

3. Rule making in favor of open society

The technological and social developments also contribute to the establishment of an "open society."[15] The aims of this openness—evolving in a perpetual process of attempts to ameliorate and correct errors—are the preservation of individual freedom as well as the ideal of political-ideological pluralism. Openness and acceptance of other approaches and solutions for problems should be available, leading to a comparative environment and allowing the best alternative to establish itself.[16] Cyberspace is particularly apt for an "open society," since new possibilities for participation may be discovered and previous involvement processes could be ameliorated.

The "openness" also presupposes that public forums are accessible and allow an exchange of opinions. This transparent scheme would allow widespread involvement of participants with different backgrounds and manifold ideas; taking note of other individuals' opinions can lead to dynamic processes being directed to new social and environmental horizons.[17] This kind of involvement is particularly important, since behind every new technology lurks someone's desire to exert control over it.[18]

Networks can be characterized as systems partly overlapping and, therefore, requiring "bridges"; freedom and power are affected by the degree of openness, i.e. by the extent "to which individuals can bob and weave between networks to achieve their designed behavior, actions/perceptions, or outcomes."[19] The relation between the freedom and the aforementioned three appearances of human activities can be deepened and combined in complex configurations depending on the democratizing environment. In preparing norms it is important to understand the level of freedom and its sources, thereby enabling the rule makers to design a structure that leads to an appropriate equilibrium between the diverging interests.

Nowadays, the openness of cyberspace is threatened by governmental and private control regimes: the security-industrial complex applying extensive surveillance measures—including by co-opting private actors—has significant potential in the hand of dictatorial regimes; its technologies of control and lobbying power, mostly obscured from public gaze, might increase over the coming decade and thereby cause serious threats to individual human freedoms in cyberspace.[20]

From the private side, the openness of cyberspace can be endangered by cryptographic means (for

example encrypted songs or movies) and the implementation of the digital rights management by rightsholders. Furthermore, openness must be ensured on the private side by restricting dominant stakeholders from blocking rival content threatening their own commercial interests (for example by transforming open platforms into "walled gardens").[21] A vigorous enforcement of the openness rules in order to maintain access to innovation is needed in times of increasing establishment of horizontal and vertical bottlenecks to distribution.

Recently, the inventor of the World Wide Web, Tim Berners-Lee, proposed to implement a "Magna Carta" in order to protect and enshrine the independence of cyberspace. The web he created 15 years ago has come under increasing attack from governments and corporate influence, making it necessary to ensure an "open, neutral" system. Berners-Lee's Magna Carta plan is supposed to be taken up as part of an initiative called "the Web we Want," which calls on people to generate a digital bill of rights and an open Internet.

Openness of cyberspace corresponds to the principle that the Internet must be seen as a public sphere encompassing multiple publics with manifold interests.[22] From this perspective, openness is also a prerequisite for combatting the fragmentation of network structures. As outlined by the European Commission, the vision for cyberspace governance must consist of a single, un-fragmented network.[23]

Thesis 3: A key objective of Internet Governance should consist of the permanent promotion of openness constituting a universal concept that enshrines free access and free communications' principles.

4. Appropriateness of multi-layer structure

In the cyberspace context, different layers have to design the framework of regulations: the basic differentiation necessary in the design concerns the facts and values of the underlying reality; this assessment leads to the distinction of descriptive and evaluative elements on the level of social norms (informal normative order) and legal norms (institutional normative order).

Multi-layer governance requires the development of common foundations applicable to all relevant layers; at the same time, it must respect diversity and pluralism in order to be commensurate with the respective level of integration. An important aspect of this movement is the acknowledgment of the need for increased cooperation when trying to achieve a multi-layer consistency.

Multi-layer governance addresses normative guidance as to how relations between different layers of governance should be framed in a coherent manner, encompassing both analytical and prospective issues in building upon observations of legal phenomena. The definition of the proper interaction of the different levels has a direct impact on an ideally coherent regulatory architecture of multi-layer governance, i.e., multi-layer governance "proposes a process and direction."[24] If common legal rights and obligations can be identified, the ensuing legal framework enjoys special legitimacy, which is essential for the operation and effectiveness of law.[25]

Since regulatory frameworks evolve within a given societal and political context, private regimes are part of the overall legal design, particularly if their weaknesses can be eliminated or at least diminished. These regimes have a certain place in a multi-layer structure, if developed with the objective of establishing an appropriate institutionalization, based on broad initiation and wide building support. Other elements are the significance of the institutional environments, the dynamics of relationships, and how non-sovereign bodies respond to multiple legitimacy claims in complex and dynamic regulatory situations. In relation to non-state or private networks and organizations, the governance emphasis should not be based on normative validity; moreover, the trend towards efficiency and public value maximization also needs to be supported.

Notwithstanding the fact that some elements that define multi-layer governance in a global context seem diffuse, important core themes can be extracted:[26]

- Future regulatory problems by their nature will require broader and more collective decision making than applied in traditional regimes; global interactions necessitate the establishment of a multistakeholder regime.
- Responses to new problems are complex on the global level, and flat structures on different sub-levels facilitate decision making by including the relevant persons and organizations in the process at the actual point of their respective concern.
- The ongoing processes of globalization and integration necessarily lead to an altered perception and notion of State sovereignty and ask for new elements of legitimacy in this respect.

The described multi-layer concept also goes hand in hand with the increasingly prevailing multistakeholder approach to Internet Governance.

Thesis 4: Multi-layer governance is necessary in order to enshrine descriptive and normative elements into the decision-building processes and to lay the ground for the realization of the multistakeholder approach.

5. Improved quality of rule making

In view of these developments, the conditions for regulatory quality and performance must be designed in a way that both socially mediated and environmental modalities can be adequately taken into account. The realization of these objectives calls for the implementation of the multi-layered concept; a proper interaction of the different levels has a direct impact on an ideally coherent regulatory architecture.

Irrespective of the implemented substantive legal principles for cyberspace, however, it is necessary to ensure that the norm setting reaches an adequate level of quality. A consensus of all concerned cyberspace actors on the rule-making body does not suffice if the norms are so defective that they do not achieve the envisaged normative objectives. Three problems are particularly noteworthy in this context:[27]

- In developing new norms, rule makers have to avoid creating conflicts with other rules that are already part of the cyberspace users' law system. Therefore, rule makers should research the norms of the concerned community and only then define the new rules that fit into the existing framework. Depending on the given circumstances, new rules may be able to modify existing norms by gradually extending their scope into the rule makers' desired direction, if this direction is not irreconcilable with the existing framework.
- Another problem consists of the concrete drafting of new rules; if cyberspace actors do not understand the wording, compliance with the rules can hardly be expected or achieved. In other words, the linguistic quality of norms is of importance; insufficient quality is a widely known issue in rule-making processes. In addition, if new rules do not take up the requirements of the socio-technological environment, obedience by cyberspace actors is not facilitated.
- A third pitfall occurs if the law is framed in terms that have no apparent connection to what the cyberspace actors actually do. If the relationship between the demands of the rule maker and the behavior of cyberspace actors is not recognizable, rejection and non-compliance by cyberspace actors are likely, since the respective new rule does not appear to be established on the basis of a meaningful concept. Only meaningful and respectful laws will not encounter resistance from the addressees of the norms (i.e., civil society).

As known from general law-making theories, an appropriate trade-off between simplicity and certainty with respect to the application of new rules is difficult to achieve; as a consequence, rule makers have to carefully assess cyberspace actors' required intentions, behaviors, and outcomes in some detail. As mentioned, another general observation consists of the acknowledgement that law should be embedded in a social concept and that law can hardly operate as a mechanism for controlling the behavior of cyberspace actors. Therefore, the purpose of a rule-making process should be to regulate functions and effects, not means.

Thesis 5: Rule-making bodies should strengthen the efforts to improve the quality of regulation in order to comply with the requirements of a legal framework that meets the needs of civil society.

6. Outlook

The concept of multi-layered governance requires common foundations applicable to all relevant layers, while at the same time it must respect diversity and pluralism by developing normative guidance as to how relations between different layers of governance should be framed in a coherent manner. Consequently, Internet Governance advocates should enlarge the interdisciplinary scope of thinking by taking into account the multi-layered regime in the further proliferation of regulatory concepts.

Notwithstanding the different perceptions of the various stakeholders in cyberspace, the principles agreed upon in the manifold fora need to be embedded into a comprehensible structure. This objective can be achieved if—apart from the technical operability—the legal interoperability is also improved. Legal interoperability is the process of making legal rules work together across jurisdictions. Whether new laws are implemented or existing laws are adjusted or reinterpreted depends on the given circumstances. In view of the increasing fragmentation of cyberspace regulation, efforts should be undertaken to achieve higher levels of legal and policy interoperability in order to reduce costs in cross-border business and to drive innovation and economic growth.[28]

Notes

1 Milton Mueller, Networks and States. The Global Politics of Internet Governance (Cambridge: The MIT Press, 2010), 9.
2 Laura DeNardis, The Global War for Internet Governance (New Haven/London: Yale University Press, 2014), 6.
3 Herbert L.A. Hart, The Concept of Law, 2nd ed. (Oxford: Oxford University Press, 1997), 55-57.
4 April Mara Major, "Norm Origin and Development in Cyberspace: Models of Cybernorm Evolution," Washington University Law Quarterly 78 (2000), 59-111, 86.
5 Rolf H. Weber, Regulatory Models for the Online World (Zürich: Springer, 2002), 32.
6 Niklas Luhmann, Das Recht der Gesellschaft (Frankfurt: Suhrkamp Verlag, 1993), 93, 187-191, 441.
7 Rolf H. Weber, "Multilayered Governance in International Financial Regulation and Supervision," Journal of International Economic Law 13 (2010), 683-704.
8 Louis H. Sullivan, "The tall office building artistically considered," Lippincott's Magazine 57, March 1896, 403-409, reproduced in: Leland M. Roth (ed.), America builds: Source Documents in American Architecture and Planning (New York: Harper Collins, 1983), 340-345, 345.
9 Andrew D. Murray, The Regulation of Cyberspace: Control in the Online Environment (Milton Park: Routledge-Cavendish, 2007), 30-35.
10 Richard Susskind, The Future of Law (Oxford: Oxford University Press, 1996), 240.
11 See Murray (supra note 9), 40.
12 Joanna Kulesza and Roy Balleste, "Science and Importance in Cyberspace: The Rise of Use Internet as a New Order in International Law," Fordham Intellectual Property, Media & Entertainment Law Journal 23 (2013), 1311-1349, 1346.
13 See Murray (supra note 9), 43.
14 See Gráinne de Búrca, Robert O. Keohane, and Charles F. Sabel, "Global Experimentalist Governance," British Journal of Political Science 2014 (forthcoming), now available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2423810.
15 Karl Popper, The Open Society and Its Enemies, (London: Princeton University Press, 1945).
16 Rolf H. Weber and Romana Weber, "Social Contract for the Internet Community? Historical and Philosophical Theories as Basis for the Inclusion of Civil Society in Internet Governance?," SCRIPT-ed 6 (2009), 90-105, 96.
17 See Weber and Weber (supra note 16), 96.
18 See Kulesza and Balleste (supra note 12), 1313.
19 Yochai Benkler, "Network Theory: Networks of Power, Degrees of Freedom," International Journal of Communication 5 (2011), 721-755.
20 Ian Brown and Christopher T. Marsden, Regulating Code: Good Governance and Better Regulation in the Information Age (Cambridge: The MIT Press, 2013), 162.
21 Salil K. Mehra, "Paradise is a walled garden? Trust, antitrust and user dynamism," George Mason Law Review 18 (2011), 889-952.
22 Rikke Frank Jørgensen, Framing the Net: The Internet and Human Rights (Cheltenham: Edward Elgar Publishing, 2013).
23 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Internet Policy and Governance: Europe's role in shaping the future of Internet Governance," COM(2014) 72 final, February 12, 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52014DC0072.
24 Thomas Cottier, "Multilayered Governance, Pluralism, and Moral Conflict," Indiana Journal of Global Legal Studies 16 (2009), 647-679, 656.
25 Weber (supra note 7), 690.
26 See Rolf H. Weber, Shaping Internet Governance: Regulatory Challenges, (Zürich: Springer, 2009).
27 See Chris Reed, Making Laws for Cyberspace (Oxford: Oxford University Press, 2012), 226-228.
28 John Palfrey and Urs Gasser, Interop: The Promise and Perils of Highly Interconnected Systems (New York: Basic Books, 2012), 177-179.